2017

Intruder Alert? How Stock Markets React to Potential IT Security Breaches: The Case of OpenSSL Heartbleed

Christian Janze
Goethe University Frankfurt, janze@wiwi.uni-frankfurt.de

30TH BLED ECONFERENCE: DIGITAL TRANSFORMATION – FROM CONNECTING THINGS TO TRANSFORMING OUR LIVES (JUNE 18 – 21, 2017, BLED, SLOVENIA)
A. Pucihar, M. Kljajić Borštnar, C. Kittl, P. Ravesteijn, R. Clarke & R. Bons

University of Maribor Press

Intruder Alert? How Stock Markets React to Potential IT Security Breaches: The Case of OpenSSL Heartbleed

CHRISTIAN JANZE

Abstract This exploratory study investigates how potential information technology security breaches affect stock prices. Previous research indicates that stock markets tend to punish firms that experience unsolicited disclosure of information and proprietary data. However, little research exists on the question of whether firms are punished for creating the mere potential for data theft. Based on the information boundary theory, we design our exploratory research model. Subsequently, we utilize a sample of 4,147 stocks of firms headquartered in 43 countries to conduct multiple event studies. We reveal a delayed adverse stock market response to potential IT security breaches as well as a discrimination among firms operating in different industries. Consequently, this work enhances the understanding of the full economic impact of information security measures by shedding light on previously neglected hidden costs.

Keywords: • Economics • Finance • Information Security • Event Study • Heartbleed •

CORRESPONDENCE ADDRESS: Christian Janze, Goethe University Frankfurt, Theodor-W.-Adorno-Platz 1, 60323 Frankfurt am Main, Germany, e-mail: janze@wiwi.uni-frankfurt.de.

https://doi.org/10.18690/978-961-286-043-1.18 ISBN 978-961-286-043-1

Available at: http://press.um.si.

1 Introduction

Hardly a day passes without reports of large-scale attacks against IT infrastructures launched by internal and external perpetrators. These attacks frequently result in the unintentional disclosure of confidential information and proprietary data (Liedtke 2014, Zetter 2013).

Previous research on the economic impact of IT security breaches on affected firms focuses on realized unsolicited disclosure of information and proprietary data (Acquisti et al. 2006, Campbell et al. 2003, Cavusoglu et al. 2004, Ettredge and Richardson 2002, Goel and Shawky 2009, Hovav and D'Arcy 2003, Kannan et al. 2007, Telang and Wattal 2007). However, we argue that it is equally likely that stock markets punish firms for creating the mere possibility of a data theft. This is because of a diminished trust in the firms' capabilities to protect sensitive data with adversarial effects on future sales and thus its stock price, which resembles the discounted value of expected future dividends (which are directly linked to sales). Thus, within this study, we examine the overall research question of the impact of potential IT security breaches on stock prices.

We draw on information boundary theory (IBT) to investigate our research question. Specifically, we study the impact of the Heartbleed vulnerability within the widely used cryptographic library OpenSSL (OpenSSL 2014a) on the value of 4,147 publicly traded firms. OpenSSL is used to secure connections in computer networks (Durumeric et al. 2014) and was enabled on approximately two-thirds of all webservers worldwide when Heartbleed was publicly announced (Goodin 2014). Examples of affected services include Facebook, Instagram, Google Search, Gmail, Youtube, Yahoo Search, Yahoo Mail and Dropbox (Mashable 2014). Our exploratory findings reveal a time-delayed response of stock markets to potential IT security breaches as well as a discrimination among firms operating in different industries.

The remaining portion of this paper is structured as follows. Section two provides background on related research, privacy theory as well as our research model. Section three provides information on our research methodology. Section four presents the results of our study and discusses its implications. Section five concludes the study.

2 Background and Research Model

2.1 Research on Realized IT Security Breaches

As summarized in Table 1, previous research can be largely divided into the impact of data & security breach announcements on firms and vulnerability disclosures on software vendors (Telang and Wattal 2007).

Table 1: Results of IT Security Related Event Studies by Covered Topic (Partially adapted from Acquisti et al. (2006) and Telang and Wattal (2007))

Topic	Time Period	Events	Event Window	CAAR (%)	Author(s)
Firms	2000-2005	79	[0, +1]	-0.58	Acquisti et al. (2006)
	1995-2000	43	[-1, +1]	-1.88	Campbell et al. (2003)
	1998-2000	66	[0, +1]	-2.00	Cavusoglu et al. (2004)
	2004-2008	168	N/A	-1.00	Goel and Shawky (2009)
	1998-2002	23	[-1, +1]	N/A	Hovav and D'Arcy (2003)
	1997-2003	72	[-1, +7]	-3.17	Kannan et al. (2007)
	Feb. 2000	115	[+1, +3]	-3.00%[2]	Ettredge and Richardson (2002)
Vendors	1999-2004	146	[0, +1]	-0.63	Telang and Wattal (2007)

First, results regarding the overall impact of security & data breach announcements are mixed. While some authors find negative cumulative average abnormal returns (CAARs) of publicly traded firms' stock prices ranging from -0.58% to -3.17% over short-horizon event windows below 10 days (Acquisti et al. 2006, Cavusoglu et al. 2004, Ettredge and Richardson 2002, Kannan et al. 2007) others don't. For example, numerous studies find limited evidence of overall abnormal price effects but strong evidence for discrimination among firm and event characteristics (Campbell et al. 2003, Ettredge and Richardson 2002, Hovav and D'Arcy 2003). Campbell et al. (2003) finds no evidence for an overall effect but strong and statistically significant support for negative effects of security breaches that involve unauthorized access to confidential data (-5.46%). Exemplary for evidence of discrimination among the type of firms are Hovav and D'Arcy (2003), who find a statistically negative CAAR of internet-centered firms only and Ettredge and Richardson (2002), who find a negative CAAR of internet-centric firms. Second, software vendors that created vulnerable products were negatively affected and experienced a CAAR of -0.63% associated with the announcement of a vulnerability within their products and services (Telang and Wattal 2007).

In summary, previous research focuses on the impact of realized IT security breaches. However, little research exists on the question whether stock markets punish firms for creating the mere potential to breach their IT security.

2.2 Heartbleed Vulnerability

On April 7th, 2014, the existence of Heartbleed, a vulnerability within the cryptographic library OpenSSL was publicly announced (Codenomicon 2014, Schneier 2014). Heartbleed is the result of an improper implementation of the Heartbeat Extension (Durumeric et al. 2014) specified in Request for Comments 6520 (RFC6520), and affects official OpenSSL versions 1.0.1 to 1.0.1f (OpenSSL 2014b). Heartbleed creates the

recurring possibility of unsolicited remote copying of small chunks of random memory content from a service without the need for any authorization or leaving any traces (Schneier 2014). Common Vulnerabilities and Exposures (CVE)-2014-0160 states that Heartbleed "allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys" (MITRE Corporation 2014).

Heartbleed was introduced to the OpenSSL codebase on December 31, 2011 (22:59:57 UTC) (Seggelmann 2012) and widely distributed on March 14th, 2012 with the release of OpenSSL version 1.01 (OpenSSL 2012). Grubb (2014) states that Heartbleed was discovered for the first time on or before March 21st, 2014 by Neel Mahta of Google Security (OpenSSL 2014b). Thus, the exploitation of fully patched services running OpenSSL was theoretically possible for approximately two years.

2.3 Research Model to Study Potential IT Security Breaches

The concept of privacy is considered to be of undisputed importance to societies of modern economies (Xu et al. 2008) and has been studied for centuries (Bélanger and Crossler 2011). However, grasping the concept of privacy is cumbersome because of its manifold definitions (Solove 2006). Acquisti et al. (2006) notes that attempts of precise definitions of privacy oftentimes "remain ambiguous, changing with the perspective of the observer", a view that is shared by Introna and Pouloudi (1999). Nevertheless, in a landmark paper called "The Right to Privacy", published in 1890 by Warren and Brandeis, the authors reasoned that the concept of privacy gradually evolved over time to "the right to be let alone" (Warren and Brandeis 1890). This view is still reflected by modern definitions with "the notion of privacy as freedom from the judgment of others" (Introna and Pouloudi 1999). Acquisti et al. (2006), defines a privacy incident roughly as a failure of mechanisms designed to protect personal information of customers', partners' or employees from threats of technical, managerial, organizational or human nature. The Heartbleed vulnerability thus represents an IT security related privacy incident.

IBT is the result of a research program to investigate the impact of monitoring and surveillance technology on the perceived privacy of workers (Stanton and Stam 2003). Xu et al. (2008) describes IBT as an explanatory framework that allows for studying social impacts of information disclosures: IBT states that people possess unique physical or virtual informational spaces. These spaces are limited by clearly defined boundaries. Attempts of external entities to cross these boundaries might be perceived as an intrusion into the informational space. The extent of this perception is dependent on situational and personal conditions (Xu et al. 2008). According to Stanton and Stam (2002), IBT represents the synthesis of three separate constructs: First, the communications boundary management theory (Petronio 1991). Second, the group value approach to organizational justice (Alder 1998, Alder and Tompkins 1997). Third, a general expectancy valence framework for privacy protection (Stone and Stone 1990). IBT is comparable to attempts of Moor (1997) to conceptualize multiple theories of privacy. IBT is in-line with the

reasoning that "the unifying feature of privacy incidents is the violation of certain expectations about how data will be handled" (Acquisti et al. 2006). Xu et al. (2008) show that IBT can be applied in an information privacy context to describe the formation of an individual's privacy concerns.

Table 2 distinguishes two groups of firms by the overall news the public announcement of Heartbleed conveyed to firm stakeholders. Group A includes firms that were protecting their webserver by a vulnerable version of OpenSSL, allowing for the exploitation of Heartbleed. Group B covers firms that were protecting their webserver with an unaffected SSL/TLS solution.

Table 2: Groups of Firms by News Heartbleed Conveyed to Stakeholders

Heartbleed Group	Webserver Protected by SSL/TLS?	Webserver Vulnerable?	News to Firms' Stakeholders
Group A	Yes	Yes	Bad News
Group B	Yes	No	Good News

Research hypotheses set H1 deals with the overall impact of potential IT security breaches within Group A and B and is based on IBT. We hypothesize that firms within Group A experience a reduction in shareholders' equity value, approximated by free-float stock prices, at the time of the public announcement of the Heartbleed vulnerability. Primarily because we assume that the announcement induced a re-assessment of firm stakeholders regarding the risk of unwanted information disclosure. This reassessment may result in a change in outcome from an acceptable- to an unacceptable risk as suggested by the IBT. This outcome is primarily driven by an increased perception of privacy intrusion induced by Heartbleed. In other words, stakeholders experienced negative news and responded with a decreased willingness to provide confidential information, which ultimately decreases business opportunity of affected firms. This reduced ability to conduct business will decrease future revenues and ultimately the amount of dividends a firm is able to pay out. Ceteris paribus (same dividend-pay-out ratios, overall growth projections and equity cost of capital) and assuming that stock prices are primarily determined by the present value of expected future dividend payments, this results in a decrease in stock value (Berk and DeMarzo 2011). The resulting research hypothesis, in which negative stock market reactions refer to falling share prices, is explicitly stated as:

H1a. Negative stock market reaction in Group A around the public disclosure of potential IT security breaches.

Additionally, we hypothesize that Group B firms experienced a positive effect on shareholders' equity valuations at the time of potential IT security breach announcements. Especially because the knowledge that the firm was not affected by Heartbleed, despite being protected by SSL/TLS – may lead to a positive outcome of the re-assessment of the risk of unwanted information disclosure. This in turn attracts new

business opportunities through stakeholders, which previously assessed the risk as unacceptable. Furthermore, it is likely that stakeholders of Group A switched to Group B after assessing the risk of Group A firms as unacceptable, which again results in an increased ability of Group B firms to conduct business. Thus, and under the same assumptions regarding the effect on future dividend payments introduced in the last paragraph, this should result in an increase in the stock price of Group B firms:

H1b. Positive stock market reaction in Group B around the public disclosure of potential IT security breaches.

IBT states that people construct personal informational spaces within boundaries that - among other things – depend on the nature of information in question. We assume that firms in different industries process different types of information, of which some are considered of greater importance than others to the overall risk-evaluation process of firm stakeholders. For example, firms in the Communications or Financial Services industry may process more confidential information than firms in the Materials sector. Thus, we hypothesize that there are industry specific differences in the outcome of the re-assessment of the risk of unwanted information disclosure, which in combination with the reasoning of the last section yields the second set of hypotheses (H2):

H2a. Existence of industry specific differences in negative stock market reaction of firms within Group A around the public disclosure of potential IT security breaches.

H2b. Existence of industry specific differences in positive stock market reaction of firms within Group B around the public disclosure of potential IT security breaches.

3 Methodology

3.1 Event Study Design

Event studies are commonly used to examine the effect of specific events on the value of firms (Konchitchki and O'Leary 2011). While MacKinlay (1997) broadly defines event studies as "using financial market data [to] measure the impact of a specific event on the value of a firm", others developed a more narrow understanding and note that "event studies examine the behavior of firms' stock prices around corporate events" (Kothari and Warner 2007).

In event studies, the timeline is divided into the estimation window, the event window and the post event window (Campbell et al. 1996). Returns are indexed in event time t, where t=0 represents the event date. Returns prior (post) the event date are typically indexed with negative (positive) integers relative to the event date (Acquisti et al. 2006, Campbell et al. 2003). At its core, event studies assess the effect of an event on the performance of a security in the event window by subtracting the expected return of a security from actual observed returns to get abnormal returns and subsequently

aggregating these over time and/or securities. Thus, the estimated abnormal return (AR)ˆ_it of a given security i at time t can be written as

$$\widehat{AR}_{it} = R_{it} - E(R_{it} \mid X_{it}),$$

where R_it represents the actual observed ex-post return and E(R_it ┤| X_t) the ex-ante normal return with X_it as the conditioning information of the normal return model (Campbell et al. 1996).

Two predominant normal return estimation models (MacKinlay 1997) are the constant mean return model and the market model, in which X_it is the market return that is the same for each security i but changes with t (Campbell et al. 1996). The market model R_it= α_i+β_i R_mt+ξ_it, linearly relates the return R_it of a security i at time t to the return R_mt of market portfolio m at time t with disturbance term ξ_it that exhibits an expected value of zero and variance σ_(ξ_i)^2 (MacKinlay 1997). Parameters of the market model are the intercept α_i and the slope β_i of security i, which can be empirically determined by means of OLS regression using estimation window data (MacKinlay 1997).
The abnormal return (AR)ˆ_it of security i at time t within the event window using the market model can then be estimated as

$$\widehat{AR}_{it} = R_{it} - \hat{\alpha}_i - \hat{\beta}_i R_{mt},$$

where αˆ_iand (βˆ_i)ˆare OLS estimators of the market model.

Event studies typically deal with more than one security and event windows that span over multiple days. Abnormal Returns (AR's) are therefore aggregated to draw overall inferences of the events' impact on returns (MacKinlay 1997), which can be done across time, across securities and both across security and time (Campbell et al. 1996). The cumulative average abnormal return (CAAR)ˆ(a,b) of n securities over a time-period within the event window spanning from t=a to b can be written as

$$\widehat{CAAR}(a,b) = \frac{1}{n}\sum_{i=1}^{n}\sum_{t=a}^{b}\widehat{AR}_{it}.$$

Empirical research indicates that stock prices are not normally distributed (Brown and Warner 1985). This is typically addressed by using non-parametric tests when analysing abnormal returns of a single day (Kolari and Pynnonen 2011). However, problems arise when non-parametric tests are applied over multiple days on a CAR basis (Cowan 1992, Kolari and Pynnonen 2010). Thus, Kolari and Pynnonen (2011) proposed a Generalized Rank (GRANK) testing procedure which in simulations outperformed previous non-parametric ranks tests and exhibits superior robustness to serial correlation and increased volatility induced by the event as well as cross-sectional correlation of returns due to

event day clustering. Additionally, GRANK often has good or higher empirical power when compared to highly popular parametric tests such as the ordinary t-test or BMP t-test. This holds true for event windows of any given length. Therefore, we rely on GRANK in the following.

3.2 Econometric Design

Table 3 summarizes the econometric design of each event study designed to put research hypotheses sets H1 and H2 to test and are repeated for good and bad news firms. The event of interest is the public announcement of the Heartbleed vulnerability within the cryptographic library OpenSSL on April 7th, 2014. The market model with daily close prices was chosen for estimating the normal returns. First, because gains from more sophisticated multi-factor models such as CAPM and APT based as Fama-French-3-Factor over statistical models are limited (MacKinlay 1997). Second, the market model is slightly less affected by cross-sectional return correlation in the presence of event-date clustering than the Fama-French-3-Factor-Model (Kolari and Pynnonen 2011). The estimation window length to estimate the regression coefficient is 200 trading days, which roughly equals the mean (median) of 52 papers including event studies in IS research originally compiled by Konchitchki and O'Leary (2011). Three different event window lengths, covering 3, 13 and 23 days respectively are applied. The short-horizon event window of three days complies with the econometric reasoning of superiority of short-horizon event windows by Konchitchki and O'Leary (2011). The medium- and long-horizon event windows are designed to capture potential information leakage prior to the event and delayed stock market reaction and act as a robustness check. Inclusion criteria are varying BICS level 1 classifications of firms and data cleaning rules. Missing close price data was replaced by applying Last Observation Carried Forward (LOCF) and subsequently Next Observation Carried Backward (NOCB) for each security with less than or equal to 20 missing observations, which equals 10% of the estimation window length. Daily returns exceeding 100% were replaced by 0% to remove very few outliers.

Table 3: Econometric Design of Event Studies

				Event Study Configuration ID																																
				ES1a	ES1b	ES1c	ES1d	ES1e	ES1f	ES1g	ES1h	ES1i	ES1j	ES1k	ES2a	ES2b	ES2c	ES2d	ES2e	ES2f	ES2g	ES2h	ES2i	ES2j	ES2k	ES3a	ES3b	ES3c	ES3d	ES3e	ES3f	ES3g	ES3h	ES3i	ES3j	ES3k
	Hypotheses Set			**H1**	**H2**										**H1**	**H2**										**H1**	**H2**									
Event Study Parameters	**Normal Return Model**	Model *(Benchmark Index)*		Market Model (MSCI World Price Index)																																
	Event Date	Calendar Time *(Event Time)*		2014-04-07 [0]																																
		Trading Days		1																																
	Estimation Window	Calendar Time	Start	2013-06-28											2013-06-21											2013-06-14										
			End	2014-04-03											2014-03-27											2014-03-20										
		Event Time		[-201,-2]											[-206, -7]											[-211, -12]										
		Trading days		200																																
	Event Window	Calendar Time	Start	2014-04-04											2014-03-28											2014-03-21										
			End	2014-04-08											2014-04-15											2014-04-22										
		Event Time		[-1, +1]											[-6, +6]											[-11, +11]										
		Trading days		3											13											23										
Inclusion Criteria	**Industries**	Communications		x	x										x	x										x	x									
		Consumer Discretionary		x		x									x		x									x		x								
		Consumer Staples		x			x								x			x								x			x							
		Energy		x				x							x				x							x				x						
		Financials		x					x						x					x						x					x					
		Health Care		x						x					x						x					x						x				
		Industrials		x							x				x							x				x							x			
		Materials		x								x			x								x			x								x		
		Technology		x									x		x									x		x									x	
		Utilities		x										x	x										x	x										x
	Data Cleaning Rules	Maximum Missing Returns		20																																
		Missing Price Data	LOCF	x																																
			NOCB	x																																
		Outlier Threshold		100%																																

4 Empirical Results and Discussion

4.1 Data Set and Descriptive Statistics

The primary inclusion criterion applied is the membership of a firm's stock in at least one of nine selected major stock indices as of June 24th, 2014. The resulting set is presented in Table 4 and includes a total of 4,873 constituents. Removing duplicate stocks that were member of more than one index lowered this number by 726 to a final number of 4,147.

Price data of all 4,147 stocks in the sample are compiled for the time-period of January 2nd, 2013 to July 21st, 2014. The total number of 1,483,352 HLOC price observations stem from Google Finance (857,447), Bloomberg Professional (527,755), Stooq (84,218) and Quandl (13,012). In addition, daily price data of MSCI World was acquired from Thompson Reuters Datastream. Meta data regarding the vulnerability of each of the 4,147 firms were compiled to assess the potential impact of the Heartbleed vulnerability on affected firms: Heartbleed, as previously shown, affected a multitude of software and hardware solutions: Webservers reached by the Fully Qualified Domain Name (FQDN) were selected as a proxy for a firm's vulnerability level. FQDNS of 4,137 of the 4,147 firms in the sample could be compiled. The remaining firms did not operate a webserver. Historic scan data from these webservers, allowing for determining each firm's vulnerability level prior to Heartbleed's public announcement on April 7th, 2014, originate from Netcraft Ltd. and are aggregated into three categories previously presented in Table 2. In addition, all of the 4,137 available FQDN's were rescanned on September 1st, 2014 using "Heartbleed-Masstest" written by Al-Bassam (2014).

Table 4: Sample Constituents by Stock Index, Coverage, Focus and Operator

Index	**Constituents**	**Coverage**	**Region**	**Operator**
Bloomberg European 500	501	Large Cap	Europe	Bloomberg L.P.
CAC 40	40	Large Cap	France	Euronext N.V.
DAX 30	30	Large Cap	Germany	Deutsche Börse AG
EURO STOXX 50	50	Large Cap	Europe	STOXX Ltd.
NASDAQ Composite	2,526	All Cap	U.S.	NASDAQ OMX Group Inc.
Nikkei-225 Stock Average	225	Large Cap	Japan	Nikkei Inc.
S&P 400	400	Mid Cap	U.S.	S&P Dow Jones Indices LLC
S&P 500	501	Large Cap	U.S.	S&P Dow Jones Indices LLC
STOXX Europe 600	600	All Cap	Europe	STOXX Ltd.
Total Constituents	4,147			

Figure 1 depicts the distribution of vulnerability levels within the total constituent sample of 4,147 firms before and after the public announcement of Heartbleed on April 7th, 2014.

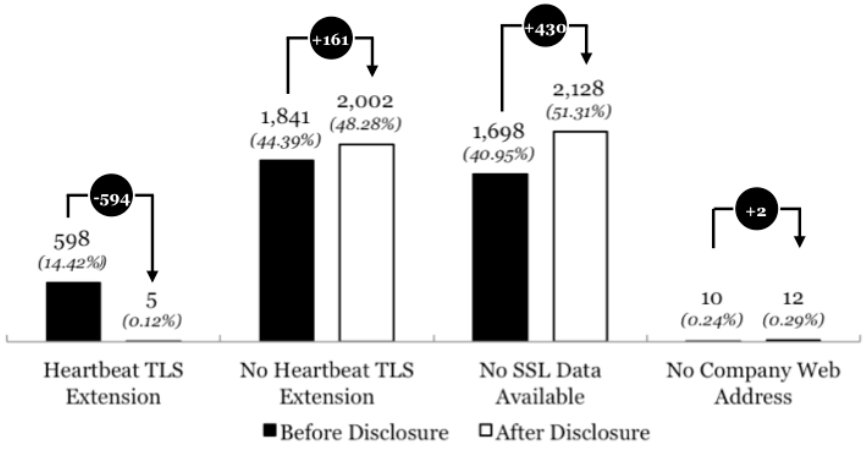

Figure 1: Distribution of Vulnerability Levels within Total Constituent Sample

4.2 Overall Impact (H1)

Hypotheses set H1 is concerned with the overall impact of potential IT security breaches on stock prices of publicly traded firms. Table 5 presents empirical results by providing CAARs and results of two-tailed non-directional GRANK-T tests over short-, medium-, and long-horizon event windows. The null hypothesis tested by the tgrank test statistic states that there is no mean effect while the alternative is that there is a mean effect (Kolari and Pynnonen 2011).

Table 5: Overall Impact of Potential IT Security Breaches on Publicly Traded Firms

Event Study	**Group A "Bad News"**				**Group B "Good News"**			
	n	**CAAR**	**t_{grank}**	**p**	**n**	**CAAR**	**t_{grank}**	**p**
ES1a (*Short-Horizon)*	538	-1.45%	1.52	0.13	1,647	-1.24%	1.39	0.17
ES2a (*Medium-Horizon)*	537	-2.94%	1.85	0.07*	1,644	-2.58%	1.81	0.07*
ES3a (*Long-Horizon)*	536	-5.28%	2.40	0.02**	1,638	-4.30%	2.32	0.02**

Hypothesis H1a predicts a negative stock market reaction in Group A around the public disclosure of potential IT security breaches. There is little empirical support of statistical significance for this prediction in the short-horizon event-window as shown in Table 5. However, in the medium- and long-horizon event windows, the Group A CAARs of -2.94% and -5.28% is of statistical significance at the 10% and 5% level respectively.

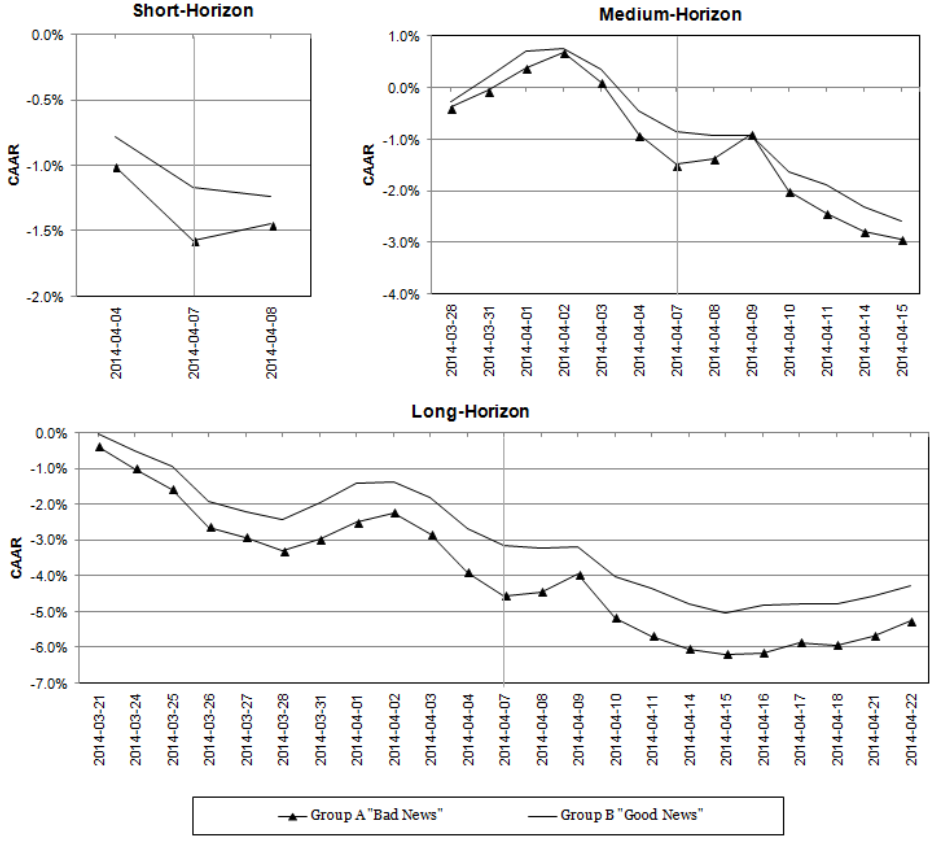

Figure 2: Impact of Potential IT Security Breaches on CAARs

Figure 2 presents the development of the overall impact of Heartbleed within each event-horizon: In the short-horizon event window, Group A firms' CAAR is most negative at the time of the public announcement of Heartbleed. Looking at the medium-horizon event window length, this recovery of Group A continues until April 9th, 2014, when the CAAR starts to drop even further. The long-horizon event window again shows the two local minima of CAAR in Group A on April 7th and April 15th, 2014 and an additional one around March 28th, 2014. Thus, we observe a time-delayed response of stock markets to potential IT security breaches.

H1b predicts a positive stock market reaction in Group B around the public disclosure of potential IT security breaches. Table 5 reveals that there is little empirical support for this prediction in the short run. The effect on firms' stock prices in Group B is negative with CAARs of -1.24%, -2.58% and -4.30% in the respective short-, medium and long-horizon event windows. While this effect was of no statistical significance in the first case, it was

in the latter two cases at the 10% and 5% level. However, Figure 2 reveals that firms in the Group B performed better, relative to firms in Group A.

4.3 Industry Specific Differences (H2)

H2a predicts the existence of industry specific differences in negative stock market reaction of firms within Group A around public disclosure of potential IT security breaches. Results presented in Table 6 seem to support this prediction. Most industry specific CAARs in the short-horizon event window are of no statistical significance according to the two-tailed GRANK-T test. However, firms operating in the Consumer Discretionary and Health Care industry experienced CAARs of -1.43 and -2.59%, which are significant at the 10% and 5% level, respectively. Interestingly, when looking at the results of the medium-horizon event window, the statistical significance of the effect on firms in the Consumer Discretionary sector vanishes. Instead, the CAAR of -4.9% of firms in the Communication sector becomes statistically significant at the 1% level. In addition, the effect on the Health Care industry becomes significant at the 1% level with a CAAR of -6.55%. In the long-horizon event window, eight out of ten industries experienced an effect of statistical significance at the 10% level ranging from CAARs of -9.47% to +4.4%.

H2b predicts the existence of industry specific differences in positive stock market reaction of firms within Group B around public disclosure of potential IT security breaches: Table 6 indicates that there is little support for this prediction in the short-horizon event window, as only the CAAR of -1.40% in the Consumer Discretionary sector is of statistical significance. Additionally, there is little support for the predicted positive effect as the vast majority of industry specific CAARs is negative. In the medium-horizon event window, three industries experienced a significant effect with CAARs ranging from -3.14 (Communications), over 3.91% (Technology) to -8.82% (Health Care). In the long-horizon event window, these negative effects increases even more. In addition, the negative effects within the Consumer Discretionary and Financials sectors are statistical significance.

Table 6: Industry Specific Impact of Potential IT Security Breaches on Stock Prices

ID	Industry	Group A				Group B			
		n	CAAR	t_{grank}	p	n	CAAR	t_{grank}	p
Short-Horizon Event Window:									
ES1a	All Industries	538	-1.45%	1.520	0.1302	1647	-1.24%	1.389	0.1665
ES1b	Communications	47	-1.91%	1.411	0.1598	101	-1.57%	1.444	0.1503
ES1c	Consumer Discretionary	129	-1.43%	1.717	0.0876*	231	-1.40%	2.043	0.0424**
ES1d	Consumer Staples	28	-2.04%	1.415	0.1587	104	0.21%	0.314	0.7536
ES1e	Energy	20	-0.02%	0.677	0.4991	76	-1.13%	0.420	0.6751
ES1f	Financials	78	-1.17%	0.901	0.3685	404	-1.00%	1.148	0.2525
ES1g	Health Care	66	-2.59%	2.237	0.0264**	173	-2.56%	1.123	0.2627
ES1h	Industrials	39	-0.88%	0.935	0.3511	182	-1.09%	1.385	0.1677
ES1i	Materials	17	-0.48%	0.443	0.6584	96	-0.34%	0.051	0.9593
ES1j	Technology	112	-1.27%	1.389	0.1663	225	-2.07%	1.582	0.1153
ES1k	Utilities	2	-0.35%	0.225	0.8220	55	0.88%	0.934	0.3513
Medium-Horizon Event Window:									
ES2a	All Industries	537	-2.94%	1.850	0.0658*	1644	-2.58%	1.809	0.0719*
ES2b	Communications	47	-4.90%	3.037	0.0027***	101	-3.14%	2.472	0.0143**
ES2c	Consumer Discretionary	129	-2.15%	1.346	0.1799	231	-2.26%	1.614	0.1081
ES2d	Consumer Staples	28	-2.40%	0.105	0.9164	104	-0.24%	0.106	0.9155
ES2e	Energy	20	2.30%	1.561	0.1200	76	0.75%	1.176	0.2412
ES2f	Financials	78	-1.88%	1.434	0.1531	403	-1.90%	1.354	0.1772
ES2g	Health Care	66	-6.55%	2.978	0.0033***	172	-8.82%	3.641	0.0003***
ES2h	Industrials	39	-0.96%	0.515	0.6075	181	-2.00%	1.162	0.2467
ES2i	Materials	17	-0.76%	0.626	0.5319	96	0.39%	0.307	0.7592
ES2j	Technology	111	-3.74%	1.638	0.1030	225	-3.91%	2.118	0.0354**
ES2k	Utilities	2	-2.26%	0.500	0.6177	55	0.89%	0.472	0.6372
Long-Horizon Event Window:									
ES3a	All Industries	536	-5.28%	2.399	0.0174**	1638	-4.30%	2.320	0.0214**
ES3b	Communications	47	-7.90%	2.632	0.0091***	101	-5.85%	3.028	0.0028***
ES3c	Consumer Discretionary	129	-4.40%	1.982	0.0488**	231	-4.27%	2.126	0.0347**
ES3d	Consumer Staples	28	-3.98%	1.269	0.2059	103	0.33%	1.170	0.2433
ES3e	Energy	20	4.40%	1.908	0.0579*	76	-0.67%	0.888	0.3757
ES3f	Financials	78	-3.74%	1.902	0.0586*	400	-4.42%	2.272	0.0242**
ES3g	Health Care	66	-9.47%	3.088	0.0023***	172	-11.16%	3.924	0.0001***
ES3h	Industrials	38	-1.74%	0.259	0.7962	179	-2.56%	1.402	0.1623
ES3i	Materials	17	-3.82%	1.940	0.0538*	96	1.95%	1.369	0.1724
ES3j	Technology	111	-7.44%	2.504	0.0131**	225	-6.88%	2.947	0.0036***
ES3k	Utilities	2	3.65%	2.628	0.0092***	55	1.12%	0.619	0.5369

Limitations of this work are primarily related to the underlying event study methodology. These can be divided into problems related to theoretical assumptions and research design (McWilliams and Siegel 1997). Theoretical assumptions are (1) efficient markets, (2) no-anticipation of the event examined and (3) the absence of confounding events

(McWilliams and Siegel 1997). First, regarding the efficient markets assumption, we assumed that people are both able to find and make sense of publicly available information. While easy to find, it is possible that firm stakeholders were unable to make sense of it due to the technical sophistication of the Heartbleed vulnerability. Thus, even if large investors were aware of the problem, they may have concluded that other stakeholders were not and assumed no re-evaluation of the risk of unintentional disclosure of private information would take place. Second, event anticipation is unlikely as search query data of Google and Wikipedia revealed no interest in Heartbleed prior its public disclosure. Third, it is not possible to control for confounding events when analyzing a sample of 4,147 firms. However, effects are likely to be wiped out due to the large sample size and are especially unlikely in the short-horizon event window where the economic calendar provided by ECONODAY reveals no event window contaminating news. Typical additional issues of event studies are the sample size, the identification of outliers, the length and justification of the event window and further explanation of abnormal returns (McWilliams and Siegel 1997). Because of the large data sample, explicitly defined outlier return thresholds, theoretically justified event windows and research hypotheses, these should not pose a significant issue. Next to these limitations, future confirmatory studies must examine comparable large scale IT security issues where a multitude of firms are affected.

5 Conclusion and Outlook

This paper provides empirical evidence on the global impact of potential IT security breaches on stock markets. Thereby, it enhances the understanding of the full economic impact of information privacy measures by shedding light on previously neglected hidden costs. By drawing on IBT, research hypotheses are developed and put to test by means of multiple large scale event studies covering 4,147 firms headquartered in 43 countries.

First, our exploratory study indicates that stock markets react with a time delay to potential IT security breaches. Second, we provide evidence for a discrimination of firms operating in different industries. Therefore, this work extends the understanding of consequences of jeopardized IT security by adding a previously neglected hidden cost component to information privacy considerations. Future scientific research in this field could investigate additional determinants of the discrimination of stock markets between potential and actual IT security breaches.

References

Acquisti A, Friedman A, Telang R (2006) Is There a Cost to Privacy Breaches? An Event Study. ICIS 2006 Proc. (Paper 94).

Al-Bassam M (2014) CVE-2014-0160 multi scanner. Retrieved (November 28, 2014), https://github.com/musalbas/heartbleed-masstest/.

Alder GS (1998) Ethical issues in electronic performance monitoring: A consideration of deontological and teleological perspectives. J. Bus. Ethics 17(7):729–743.

Alder GS, Tompkins PK (1997) Electronic Performance Monitoring: An Organizational Justice and Concertive Control Perspective. Manag. Commun. Q. 10(3):259–288.

Bélanger F, Crossler RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Q. 35(4):1017–1042.

Berk J, DeMarzo P (2011) Corporate Finance 2nd Global Edition. (Pearson Education Limited, Boston ; Munich u.a.).

Brown SJ, Warner JB (1985) Using daily stock returns: The case of event studies. J. Financ. Econ. 14(1):3–31.

Campbell JY, Lo AW, MacKinlay AC (1996) The Econometrics of Financial Markets (Princeton University Press, Princeton, N.J).

Campbell K, Gordon LA, Loeb MP, Zhou L (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J. Comput. Secur. 11(3):431–448.

Cavusoglu H, Mishra B, Raghunathan S (2004) The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. Int. J. Electron. Commer. 9(1):70–104.

Codenomicon (2014) Heartbleed Bug. Retrieved (August 27, 2014), http://heartbleed.com/.

Cowan AR (1992) Nonparametric event study tests. Rev. Quant. Finance Account. 2(4):343–358.

Durumeric Z, Kasten J, Adrian D, Halderman JA, Bailey M, Li F, Weaver N, et al. (2014) The Matter of Heartbleed. ACM Internet Meas. Conf. IMC.

Ettredge M, Richardson VJ (2002) Assessing the Risk in E-Commerce. Proc. 35th Hawaii Int. Conf. Syst. Sci. 194–194.

Goel S, Shawky HA (2009) Estimating the market impact of security breach announcements on firm values. Inf. Manage. 46(7):404–410.

Goodin D (2014) Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping. Ars Tech. Retrieved (September 22, 2014), http://arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping/.

Grubb B (2014) Heartbleed disclosure timeline: who knew what and when. Syd. Morning Her. Retrieved (October 17, 2014), http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html.

Hovav A, D'Arcy J (2003) The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. Risk Manag. Insur. Rev. 6(2):97–121.

Introna L, Pouloudi A (1999) Privacy in the Information Age: Stakeholders, Interests and Values. J. Bus. Ethics 22(1):27–38.

Kannan K, Rees J, Sridhar S (2007) Market Reactions to Information Security Breach Announcements: An Empirical Analysis. Int. J. Electron. Commer. 12(1):69–91.

Kolari JW, Pynnonen S (2010) Event Study Testing with Cross-sectional Correlation of Abnormal Returns. Rev. Financ. Stud. 23(11):3996–4025.

Kolari JW, Pynnonen S (2011) Nonparametric rank tests for event studies. J. Empir. Finance 18(5):953–971.

Konchitchki Y, O'Leary DE (2011) Event study methodologies in information systems research. Int. J. Account. Inf. Syst. 12(2):99–115.

Kothari SP, Warner JB (2007) Econometrics of Event Studies. Eckbo BE, ed. Handb. Corp. Finance Empir. Corp. Finance Vol. 1. (Elsevier), 3–36.

Liedtke M (2014) 76M households hit by JPMorgan data breach. Wall Str. J. Retrieved (October 6, 2014), http://online.wsj.com/article/AP034ca44ad33f4c888fa1b26988ce76cf.html.

MacKinlay AC (1997) Event Studies in Economics and Finance. J. Econ. Lit. 35(1):13–39.

Mashable (2014) The Heartbleed Hit List: The Passwords You Need to Change Right Now. Mashable. Retrieved (November 14, 2014), http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/.

McWilliams A, Siegel D (1997) Event Studies in Management Research: Theoretical and Empirical Issues. Acad. Manage. J. 40(3):626–657.

MITRE Corporation (2014) CVE-2014-0160. MITRE Common Vulnerabilities Expo. Retrieved (August 27, 2014), https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160.

Moor JH (1997) Towards a Theory of Privacy in the Information Age. Comput. Soc. 27(3):27–32.

OpenSSL (2012) OpenSSL CHANGES. Retrieved (September 22, 2014), http://git.openssl.org/gitweb/?p=openssl.git;a=blob_plain;f=CHANGES;hb=refs/heads/OpenSSL_1_0_1-stable.

OpenSSL (2014a) About the OpenSSL Project. Retrieved (October 20, 2014), https://www.openssl.org/about/.

OpenSSL (2014b) OpenSSL vulnerabilities. Retrieved (August 27, 2014), https://www.openssl.org/news/vulnerabilities.html#2014-0160.

Petronio S (1991) Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. Commun. Theory 1(4):311–335.

Schneier B (2014) Heartbleed. Schneier Secur. Retrieved (August 29, 2014), https://www.schneier.com/blog/archives/2014/04/heartbleed.html.

Seggelmann R (2012) projects/openssl.git/commit. OpenSSL. Retrieved (September 22, 2014), http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=4817504d069b4c5082161b02a22116ad75f822b1.

Solove DJ (2006) A taxonomy of privacy. Univ. Pa. Law Rev.:477–564.

Stanton JM, Stam KR (2003) Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. Surveill. Soc. 1(2):152–190.

Stone EF, Stone DL (1990) Privacy in organizations: theoretical issues, research findings and protection mechanisms. Res. Pers. Hum. Resour. Manag. (8):349–411.

Telang R, Wattal S (2007) An Empirical Analysis of the Impact of Software Vulnerability Announcements On Firm Stock Price. IEEE Trans. Softw. Eng. 33(8):544–557.

Warren SD, Brandeis LD (1890) The Right to Privacy. Harv. Law Rev. 4(5):193–220.

Xu H, Dinev T, Smith HJ, Hart P (2008) Examining the formation of individual's privacy concerns: toward an integrative view. ICIS 2008 Proc. (Paper 6).

Zetter K (2013) Target Admits Massive Credit Card Breach; 40 Million Affected | WIRED. Retrieved (October 7, 2014), http://www.wired.com/2013/12/target-hack-hits-40-million/.